

# Elliptic-Curves Cryptography on High-Dimensional Surfaces

Alberto Sonnino<sup>1</sup> and Giorgio Sonnino<sup>2,3</sup>

(1) Department of Computer Sciences,  
University College London (UCL), London, UK  
Email: alberto.sonnino.15@ucl.ac.uk

(2) Department of Theoretical Physics and Mathematics,  
Université Libre de Bruxelles (U.L.B.),  
Campus Plaine C.P. 231, 1050 Brussels - Belgium

(3) Royal Military School (RMS),  
Av. de la Renaissance 30, 1000 Brussels - Belgium  
Email: gsonnino@ulb.ac.be

## Abstract

We discuss the use of elliptic curves in cryptography on high-dimensional surfaces. In particular, instead of a Diffie-Hellman key exchange protocol written in the form of a bi-dimensional row, where the elements are made up with 256 bits, we propose a key exchange protocol given in a matrix form, with four independent entries each of them constructed with 64 bits. Apart from the great advantage of significantly reducing the number of used bits, this methodology appears to be immune to attacks of the style of Western, Miller, and Adleman, and at the same time it is also able to reach the same level of security as the cryptographic system presently obtained by the Microsoft Digital Rights Management. A nonlinear differential equation (NDE) admitting the elliptic curves as a special case is also proposed. The study of the class of solutions of this NDE is in progress.

Keywords: Elliptic-curve cryptography, Elliptic-curve discrete log problem, Public key cryptography, Nonlinear differential equations.

## 1 Introduction

As known, encryption is the conversion of electronic data into another form, called *ciphertext*, which cannot be easily understood by anyone except authorized parties. The primary purpose of encryption is to protect the confidentiality of digital data

stored on computer systems or transmitted via the Internet or other computer networks. Encryption algorithms can provide not only confidentiality, but also authentication (i.e., the origin message is verified), integrity (i.e., the contents of the message have not been changed), and non-repudiation (i.e., the sender cannot deny to be the author of the message) [1, 2]. Elliptic curves are more and more used in cryptography [3, 4]. Their main advantage is that shorter encryption keys use fewer memory and CPU resources for achieving the same level of security than traditional methods [5]. The main concept behind this is the use of the so-called *one-way functions*. A one-way function is a function for which it is relatively easy to compute the image of some elements in the domain but it is extremely difficult to reverse this process and determine the original element solely based on the given image [6]. More precisely, according to the Federal Office for Information Security (BSI) [7], the *recommended security parameters for elliptic curves is 256 bits* (standards for the years 2017-2021). However, to manipulate data with this degree of security is computationally expensive and often impossible on embedded systems. At present many industrial systems adopt (much) less secure methodologies. This necessitates a re-evaluation of our cryptographic strategy. The question is: *are we able to obtain the same degree of security with small embedded microprocessors managing only 64-bit operations?* The solution of this problem entails several steps:

**A)** First step: *Research*

The solution of this problem requires new mathematical concepts and algorithms.

**B)** Second step: *Commercialization*

Once found the solution, the process is concluded with the start-up of the commercialization of the product.

This manuscript deals only with the first step. We shall introduce a hyper-surface in an arbitrary  $(n^2 + 1)$ -dimensional space (with  $n$  denoting a positive integer number), and we use the idea of the *one-way function* possessing also the property of being a *trap function*. The encrypted shared-key, instead to be written as a (very large) scalar number is brought into a matrix form. We shall prove that we may obtain the same degree of security as the one obtained by the Microsoft Digital Rights Management [8] by sending an encrypted shared-matrix with four independent entries, each of them made up by 64 bits. The encrypted information is successively transmitted through elliptic curves obtained by projecting the hyper-surface imbedded in a  $(n^2 + 1)$ -dimensional space onto perpendicular planes. This methodology allows reaching the same level of security as the cryptographic system presently obtained by the Microsoft Digital Rights Management.

The manuscript is organized as follows. In Section (2) we introduce high-dimensional surfaces cryptography (HDSC) and the elliptic curves constructed through these hyper-surfaces. Without loss of generality, we shall limit ourselves to the case of  $n = 2$  (i.e., to a 5D-space). The generalization to  $(n^2 + 1)$ -dimensional space is straightforward. The definition of the groups in elliptic curves on high-dimensional surfaces and the elliptic curve discrete log problem can be found in the Subsections (2.1) and (2.2), respectively. Concluding remarks are reported in the Section (4).

## 2 Elliptic-Curves Cryptography on High Dimensional Surfaces

We illustrate the methodology by dealing with a five-dimensional elliptic curve, even though the procedure is straightforwardly generalizable to elliptic curves on surfaces imbedded in an arbitrary  $(n^2 + 1)$ -dimensional space, with  $n$  denoting a positive integer number (the reason for which only spaces of such dimension are allowed will soon be clear). For the sake of simplicity, in this work we shall limit ourselves to the analysis of elliptic curves on 5-dimensional surfaces. The generalization to the general case (i.e., to the case of elliptic curves on  $(n^2 + 1)$ -hyper-surface) is straightforward<sup>1</sup>. In a 5-dimensional space, the surfaces on which the elliptic curves are defined, are the solutions of the equation

$$E = \left\{ (y, x_1, x_2, x_3, x_4) \mid y^2 = x_1^3 + x_2^3 + x_3^3 + x_4^3 + \mathbf{A} \cdot \mathbf{X} + b \right\} \quad \text{where} \quad (1)$$

$$\mathbf{A} \equiv (a_1, a_2, a_3, a_4) \quad ; \quad \mathbf{X} \equiv \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

with  $a_i$  ( $i = 1, \dots, 4$ ) and  $b$  denoting elements of the field  $\mathbb{K}$ . Examples of fields  $\mathbb{K}$  are the Real Numbers,  $\mathbb{R}$ , the Rational Numbers,  $\mathbb{Q}$ , the Complex Numbers,  $\mathbb{C}$  or the Integers modulo  $p$ ,  $\mathbb{Z}/p\mathbb{Z}$ . By fixing three of the four variables  $x_i$  (by setting, for example,  $x_2 = c_2 = \text{const.}$ ,  $x_3 = c_3 = \text{const.}$  and  $x_4 = c_4 = \text{const.}$ ) and by rotating the indexes, Eq. (1) defines together with the *points at infinity*  $\mathcal{O}$ , four distinguished two-dimensional elliptic curves  $E_i$ :

$$E_i = \left\{ (y, x_i) \mid y^2 = x_i^3 + a_i x_i + b_i \right\} \cup \{ \mathcal{O} \} \quad \text{with} \quad i = (1, \dots, 4) \quad \text{and} \quad (2)$$

$$b_1 \equiv b + c_2^3 + c_3^3 + c_4^3 + a_2 c_2 + a_3 c_3 + a_4 c_4$$

$$b_2 \equiv b + c_1^3 + c_3^3 + c_4^3 + a_1 c_1 + a_3 c_3 + a_4 c_4$$

$$b_3 \equiv b + c_1^3 + c_2^3 + c_4^3 + a_1 c_1 + a_2 c_2 + a_4 c_4$$

$$b_4 \equiv b + c_1^3 + c_2^3 + c_3^3 + a_1 c_1 + a_2 c_2 + a_3 c_3$$

being  $c_i$  ( $i = 1 \dots 4$ ) elements of  $\mathbb{K}$ . In order to avoid degeneracy, these parameters are subject to the following restrictions

$$\begin{aligned} 4a_1^3 + 27(b + c_2^3 + c_3^3 + c_4^3 + a_2 c_2 + a_3 c_3 + a_4 c_4)^2 &\neq 0 \\ 4a_2^3 + 27(b + c_1^3 + c_3^3 + c_4^3 + a_1 c_1 + a_3 c_3 + a_4 c_4)^2 &\neq 0 \\ 4a_3^3 + 27(b + c_1^3 + c_2^3 + c_4^3 + a_1 c_1 + a_2 c_2 + a_4 c_4)^2 &\neq 0 \\ 4a_4^3 + 27(b + c_1^3 + c_2^3 + c_3^3 + a_1 c_1 + a_2 c_2 + a_3 c_3)^2 &\neq 0 \end{aligned} \quad (3)$$

Clearly, in case of  $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ , we may associate four modules  $p$  to each elliptic curves. As we shall see in the forthcoming section, only elliptic curves on hyper-surfaces of dimension  $n^2 + 1$  (with  $n =$  denoting a positive integer number) are acceptable

---

<sup>1</sup>In fact, we anticipate that the encrypted code involves only square matrices of order  $n \times n$  - see next Section.

since the shared-key involves only square matrices of order  $n \times n$ . For illustration purpose only, Figure 1 shows a three dimensional surface where the values of the parameters are  $a_1 = -4$ ,  $a_2 = -5$  and  $b = 3.5$ . Figures 2 and 3 refer to the elliptic curves obtained by projecting the surface 1 onto the planes  $x_1 = 1$  and  $x_2 = -2$ , respectively.

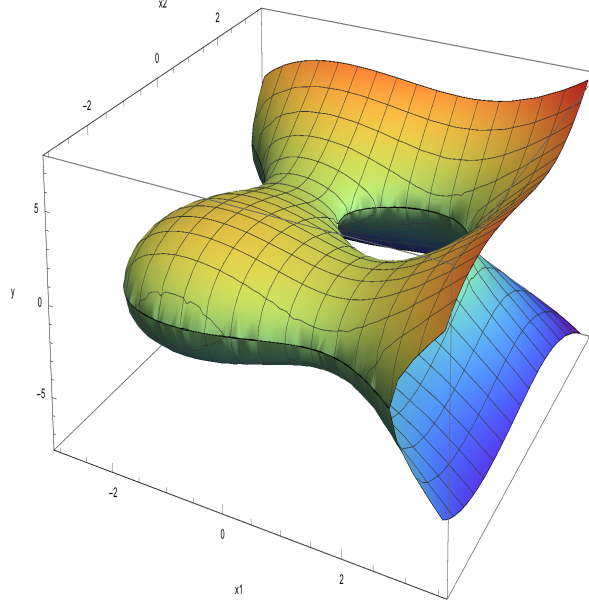


Figure 1: Only for illustration purpose, we show the two-dimensional surface given by Eq. (2) with parameters  $a_1 = -4$ ,  $a_2 = -5$  and  $b = 3.5$ . However, one should bear in mind that only elliptic curves on hyper-surfaces of dimension  $n^2 + 1$  have real meaning (hence, only elliptic curves constructed by hyper-surfaces of dimensions 2, 5, 10 and so on, are acceptable). This because, as we shall see in the forthcoming section, the encrypted code involves only square matrices of order  $n \times n$ .

## 2.1 Groups in Elliptic Curves on High-Dimensional Surfaces

Each elliptic curve  $E_i$ , separately, defines under point addition an abelian group. For each  $P_i \in E_i$ ,  $Q_i \in E_i$  and  $R_i \in E_i$  the following properties are satisfied:

- *Commutative* :  $P_i + Q_i = Q_i + P_i$ .
- *Identity* :  $P_i + \mathcal{O} = \mathcal{O} + P_i = P_i$ ;
- *Inverse* :  $P_i - P_i = P_i + (-P_i) = \mathcal{O}$ ;
- *Associative* :  $P_i + (Q_i + R_i) = (P_i + Q_i) + R_i$ ;
- *Closed* : If  $P_i \in E_i$  and  $Q_i \in E_i$ , then  $P_i + Q_i \in E_i$ ;

Each group identified by  $E_i$  is equipped with the standard *group operations* [9, 10], i.e.

- *Addition* - If  $P_i = (P_{ix_i}, P_{iy}) \in E_i$  and  $Q_i = (Q_{ix_i}, Q_{iy}) \in E_i$ , then  $P_i + Q_i = R_i$

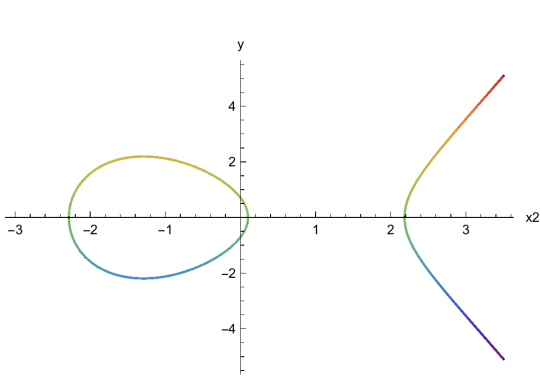


Figure 2: Elliptic curve obtained by projecting the surface 1 onto the plane  $x_1 = 1$ .

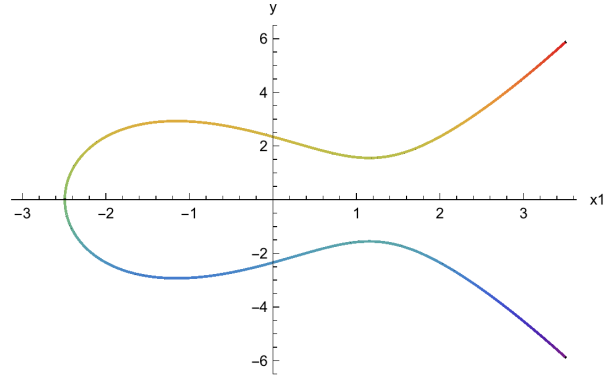


Figure 3: Elliptic curve obtained by projecting the surface 1 onto the plane  $x_2 = -2$ .

[with  $R_i = (R_{ix_i}, R_{iy})$ ], which algebraically is defined as

$$\begin{aligned} R_{ix_i} &= s_i^2 - (P_{ix_i} + Q_{ix_i}) \\ R_{iy} &= s_i(P_{ix_i} - R_{ix_i}) - P_{iy} \\ s_i &= \frac{P_{iy} - Q_{iy}}{P_{ix_i} - Q_{ix_i}} \end{aligned} \quad (4)$$

for  $i = (1, \dots, 4)$ . As a particular case, we get  $2P$ :

$$\begin{aligned} 2P_{ix_i} &= s_i^2 - 2P_{ix_i} \\ 2P_{iy} &= s_i(P_{ix_i} - R_{ix_i}) - P_{iy} \\ s_i &= \frac{3P_{ix_i}^2 + a_i}{2P_{iy}} \end{aligned} \quad (5)$$

with  $i = (1, \dots, 4)$ . The points at infinity are reached in each elliptic curves  $E_i$  when  $P_i + Q_i = \mathcal{O}$  if  $P_{ix_i} = Q_{ix_i}$  or when  $y = 0$  for point doubling (i.e.,  $P_i + P_i = \mathcal{O}$ ).

- *Scalar Multiplication* - If  $P \in E_i$  and  $\kappa \in \mathbb{Z}$ , Eq. (5) allows defining the operation  $Q = \kappa P$  under the condition that the operation  $Q = \kappa P \equiv P + \dots + P$ , equal  $\kappa$  times  $P$ , is performed by using the *same* elliptic curve  $E_i$  i.e.,  $Q \in E_i$ . The scalar multiplication defines the *one-way function*  $Q \rightarrow P$  where is very difficult to extract the value of  $\kappa$ .

- *Reflection* - The reflection of a point is its inverse. Hence for  $P_i = (P_{ix_i}, P_{iy})$  the inverse of  $P_i$  is  $-P_i = (P_{ix_i}, -P_{iy})$  satisfying the relation  $P_i - P_i = \mathcal{O}$ .

## 2.2 High-Dimensional Elliptic Curve Discrete Log Problem

For each  $E_i$  the scalar multiplication defines a *one way-function* [11]. Let us consider elliptic curves  $E_i(\mathbb{Z}/p_i\mathbb{Z})$ , with  $p_i = (p_1, \dots, p_4)$ , and let and et  $Q_1$  and  $P_1$  two points belonging to the same elliptic curve, say  $E_1$ , with the condition that  $Q_1$  is a multiple of  $P_1$ . As know, to find the value of the number  $\kappa$  such that  $Q_1 = \kappa P_1$  is a very difficult problem [12]. We introduce now the first *base point* (*Generator*),

$G_1 \equiv (G_{x_1}, G_y) \in E_1(\mathbb{Z}/p_1\mathbb{Z})$ . Since the group is *closed*,  $G_1$  generates a *cyclic group* under point addition in the curve  $E_1$ . The order  $n_1$  (with  $n_1 \in \mathbb{K}$ ) of  $G_1$  is the number of the points in the group that  $G_1$  generates. By this operation, we say that  $G_1$  generates a subgroup of size  $n$ , and we write  $\text{ord}(G_1) = n_1$ . The *order of the subgroup* generated by  $G_1$  is the smallest integer  $\kappa_1$  such that  $\kappa_1 G_1 = \mathcal{O}$  (hence,  $n_1 < \kappa_1$ ).

After  $n_1$  iterations on the curve  $E_1$  we find a second *base point (Generator)*,  $G_2$  with coordinates  $G_2(n_1) = [G_{x_2}(n_1), G_{y_2}(n_1)]$ . We may keep this second generator to perform  $n_2$  iterations on the curve  $E_2$ , with  $n_2 < \kappa_2$  being  $\kappa_2$  the order of the subgroup generated by  $G_2$  on the elliptic curve  $E_2$ . After  $n_2$  iterations we get a third *base point (Generator)*,  $G_3$  with coordinates  $G_3(n_2) = [G_{x_3}(n_2), G_{y_3}(n_2)]$ . With this second generator we perform  $n_3$  iterations on the curve  $E_3$ , with  $n_3 < \kappa_3$  (with  $\kappa$  denoting the order of the subgroup generated by  $G_3$  on the elliptic curve  $E_3$ ). After  $n_3$  iterations on the curve  $E_3$  we get the fourth *base point (Generator)*,  $G_4$  with coordinates  $G_4(n_3) = [G_{x_4}(n_3), G_{y_4}(n_3)]$ . The process concludes after  $n_4$  iterations on the elliptic curves  $E_4$  (with  $n_4$  less than  $\kappa_4$ , the order of the subgroup generated by  $G_3$  on the curve  $E_4$ ). At the end of these operations we get three matrices  $N$ ,  $G$  and  $K$ , of order  $2 \times 2$ , where the entries are totally *independent from each others*. Matrices  $N$  and  $G$  reads<sup>2</sup>

$$N = \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} \quad ; \quad G = \begin{pmatrix} G_{x_1} & G_{x_2}(n_1) \\ G_{x_3}(n_2) & G_{x_4}(n_3) \end{pmatrix} \quad ; \quad K = \begin{pmatrix} \kappa_1 & \kappa_2 \\ \kappa_3 & \kappa_4 \end{pmatrix} \quad (6)$$

The parameters that also *Eve*, the eavesdropper, possesses are  $(p_i, a_i, b_i, G, K)$  with  $i = (1, \dots, 4)$ .  $p_i$  specify the modulo of the fields  $\mathbb{K}_i$ ,  $a_i$  and  $b_i$  define the elliptic curves  $E_i$  (notice that in general these curves are different from each others),  $G$  is the Generator matrix and  $K$  is the order of the subgroups generated by  $G$ , respectively. Now, if *Bob* and *Alice* want to communicate with each other, *Bob* picks private key  $N$  with  $1 \leq n_i \leq \kappa_i - 1$ ,  $i = (1, \dots, 4)$ . *Bob* computes matrix  $T = NG$ , which belongs to the curves  $E$  [given by Eq. (1)]. At the same time, *Alice* picks private key  $M$

$$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \quad (7)$$

where the entries  $m_i$  satisfy the conditions  $1 \leq m_i \leq \kappa_i - 1$ ,  $i = (1, \dots, 4)$ . *Alice* receives from *Bob* the information  $T$  and she generates the point  $MT = MGN = W$  (notice that matrices do not commute). *Bob* receives from *Alice* the information  $P = MG$  and he computes  $PN = MGN = W$ <sup>3</sup>. Both players, *Bob* and *Alice*, possess the same (encrypted) key  $W$ , which also belongs to the curve  $E$  [given by Eq. (1)]. *Eve*, the eavesdropper, sees both information  $T$  and  $P$ , but he is unable to retrieve the sheared-key  $W$ . Figure 4 depicts the entire process.

- *Eve* does not know to which entry of the matrix  $G$  the generators have been assigned;
- In case of  $5D$ -elliptic curves, the process runs on four, distinguished and independent,  $2D$ -elliptic curves and the encrypted key belongs to a  $5D$ -surface. This

<sup>2</sup>Note that, once generated, the elements  $G_{x_1}, G_{x_i}(n_i)$  may be allocated as entries of the matrix  $G$  in a random way.

<sup>3</sup>Note that *Bob* multiplies matrices by placing  $N$  always on the right, while *Alice* multiplies matrices by placing  $M$  always on the left.

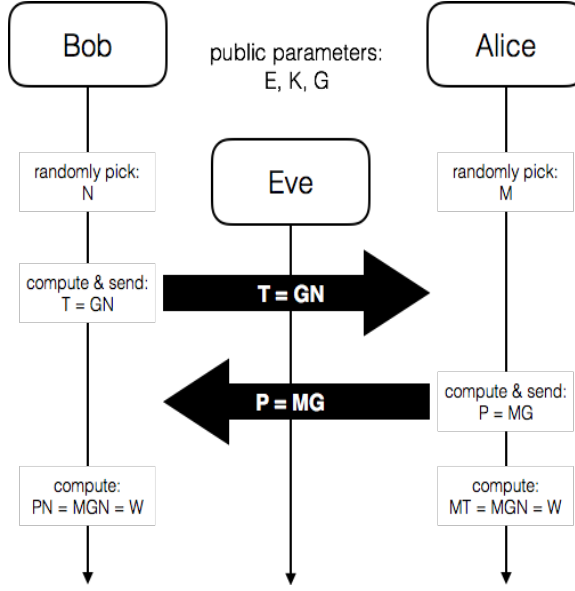


Figure 4: Diffie-Hellman key exchange protocol [13] in high-dimensional elliptic curves cryptography. *Bob* and *Alice* exchange the encryption key in a matrix form,  $W = MGN$ , having four independent entries each of them constructed with 64 bits. *Eve*, the eavesdropper, may see  $T = GN$  and  $P = MG$ , but he is unable to decrypt the sheared *Bob-Alice's* key  $W$  since it is very difficult to reverse the process and determine what was the original information.

hyper-surface is constructed in such a way that the curves with variables  $x_i$ , obtained by setting constant the remaining variables of this hyper-surface (i.e., by setting  $x_j = \text{const.}$  with  $j \neq i$ ), are elliptic curves;

- The level of security remains unchanged. Indeed, it is easily to convince ourselves that to obtain the same level of security as in case of one-dimensional elliptic curve cryptography (which requires 256 bits), we need to encode the shared-key with only 64 bits elements (since in our case, for a shared-key written in the form of a matrix  $2 \times 2$  the level of security is of the order of  $\alpha^4$ , with  $\alpha$  denoting the number of required bits).

We recall that the present methodology applies to elliptic curves cryptography constructed on hyper-surfaces of dimension  $n^2 + 1$  (with  $n$  denoting an integer number) because the shared-key is brought into the form of  $n \times n$  square matrices. Hence, a surface like Eq. (1) is the immediate generalization of a one-dimensional elliptic curves cryptography. The subsequent surface which generalizes Eq. (1) should be imbedded in a ten-dimensional space, and so on.

### 3 Examples of Practical Uses of High- Dimensional Elliptic Curve Cryptography

The aim of this section is to illustrate the many possibilities and practical usages opened by the introduction of High-Dimensional Elliptic Curve Cryptography. Gen-

erally speaking, HDECC can be applied instead of any use of the classic ECC; i.e., Bitcoin, secure shell (*ssl*), transport layer security (*tls*) [14]. Among these applications, one of the most important is certainly *tls*. Indeed, *tls* is the new generation of the Secure Socket Layer (*ssl*) which is used in any modern telecommunication. For instance, the well-known *https* is nothing else than the classic *http* protocol running within *ssl/tls* in order to ensure a secured, bidirectional connection for arbitrary binary data between two hosts. In order to establish a shared key between these two hosts, the current implementations of *tls* mainly relies on the DH or ECDH key exchange protocols discussed in the previous sections.

However, introducing such security layers comes at the price of overheads in terms of infrastructure costs, communication latency, data usage, and energy consumption [15]. Therefore, the first motivation of HDECC is to reduce the cost of security in many of the today's state-of-the-art communication technologies. Moreover, reducing these costs makes the most modern security protocols accessible for embedded systems and wearable devices. Indeed, by using HDECC, we could reduce the cost of these protocols by performing operations on data four time shorter than before by maintaining, at the same time, the same level of security. In addition, HDECC opens new perspectives on elliptic curve cryptography as we shall discuss in the next section.

## 4 Conclusion and Perspectives

We have proposed an encrypted procedure based on the high-dimensional elliptic curve cryptography, which allows maintaining the same level of security as presently obtained by the Microsoft Digital Rights Management. The advantages of these methodology are multiplex.

- 1) The quite heavy intermediate exponential operations are avoided and the key exchange protocol is constructed with 64 bits operations instead of 256 bits.
- 2) We may proceed to the construct of a new generation of cryptographic standards working with the technology *high-dimensional elliptic curves*.
- 3) This methodology opens new perspectives. In fact it is not difficult to derive a nonlinear differential equation (NDE) admitting the elliptic curves by a special choice of the parameters and initial conditions. We get

$$\begin{aligned} y'' + \alpha_1(x)y^{-1/2}y'' + \alpha_2(x)y^{-1/2}y' + \alpha_3(x)y^{-3/2}y'^2 + \alpha_4(x) &= 0 \\ y(0) = \beta_1 \quad ; \quad y'(0) = \beta_2 \\ \text{with } \alpha_i(x) = a_i + b_i x \quad (i = 1, 2, 3, 4) \quad \text{and} \quad a_i, b_i, \beta_1, \beta_2 = \text{const.} \end{aligned} \quad (8)$$

with  $'$  denoting the derivative with respect to the variable  $x$ . Note that the differential equation (8) admits as a special solution the *Weierstrass equation* [16]

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6 \quad (9)$$

with  $c_i \in K$ . If  $\text{Char}K \neq (2, 3)$ , we can complete before the square and, successively, the cube, by defining

$$\eta = y + (c_1x + c_3)/2 \quad ; \quad \xi = x + (c_1^2 + 4c_2)/12 \quad (10)$$



By substituting Eqs (10) into Eq. (9), we get the *elliptic curve* [17]:

$$\eta^2 = \xi^3 - \frac{d_4}{48}\xi - \frac{d_6}{864} \quad (11)$$

where

$$\begin{aligned} d_4 &= (c_1^2 + 4c_2)^2 - 24(c_1c_3 + 2c_4) \\ d_6 &= -(c_1^2 + 4c_2)^3 + 36(c_1^2 + 4c_2)(c_1c_3 + 2c_4) - 216(c_3^2 + 4c_6) \end{aligned} \quad (12)$$

Clearly, now the question is: *how can we determine the largest class of parameters  $a_i$ ,  $b_i$ ,  $\beta_1$  and  $\beta_2$ , introduced in (8), such that the NDE (8) admits (only) a class of one-way functions, possessing the property of being trap functions?* In addition, we should also be able to define on these curves a group under point addition. Successively, the trapped curves could be identified uniquely by indexes. Being able to answer to this question would allow encrypting not only the key exchange protocol but also the trapped-curves on which the generator and the encrypted keys belong. However, all of this requires sophisticated mathematical tools and it will be subject of future works.

We close this Section by mentioning other two relevant perspectives of this work.

i) It is quite evident that the formalism illustrated in this manuscript allows introducing two operations: *matrix addition* and *scalar matrix multiplication* (including the so-called *matrix doubling operation*). These operations can be used to implement a high-dimensional version of algorithms such as the ECDSA (elliptic curves digital signature algorithm) [18].

ii) It is possible to introduce an operator  $\mathcal{L}$  which connects two distinct points  $G^{(1)}$ ,  $G^{(2)}$  on the high-dimensional surface  $E$  [see Eq. (1)] as follows

$$G^{(1)} = \mathcal{L}G^{(2)} \implies \begin{pmatrix} G_{x_1}^{(1)} & G_{x_2}^{(1)}(n_1) \\ G_{x_3}^{(1)}(n_2) & G_{x_4}^{(1)}(n_3) \end{pmatrix} = \mathcal{L} \begin{pmatrix} G_{x_1}^{(2)} & G_{x_2}^{(2)}(n_4) \\ G_{x_3}^{(2)}(n_5) & G_{x_4}^{(2)}(n_6) \end{pmatrix} \quad (13)$$

with  $\mathcal{L}$  denoting a non-singular  $2 \times 2$  matrix, satisfying the group law under matrix multiplication. The analytic expression and the mathematical study of this matrix (and the  $n \times n$  matrices, in general), with its potential application in cryptography, will be subject of a future work.

## 5 Acknowledgments

AS is indebted with Prof. G. Danezis, from University College London (UCL), Department of Computer Sciences, and Prof. J. Becker, from Karlsruhe Institute of Technology (KIT), Institut für Technik der Informationsverarbeitung (ITIV), for their support and useful suggestions. GS is also very grateful to Prof. Pasquale Nardone and Dr Philippe Peeters from the Université Libre de Bruxelles (U.L.B.).

## References

- [1] R. Anderson, *Security Engineering*, Wiley Publishing Inc, Second Edition, 2008.

- [2] WhatIs.com - SearchSecurity, *What is encryption ?* This definition is part of the *Essential Guide to business continuity and disaster recovery plans*, <http://searchdisasterrecovery.techtarget.com/essentialguide/Essential-guide-to-business-continuity-and-disaster-recovery-plans>.
- [3] V. S. Miller, *Use of Elliptic Curves in Cryptography*, *Lecture Notes in Computer Science*, **218**, pp. 417-426 (2000).
- [4] V. Kapoor, V. Sonny Abraham, R. Singh, *Elliptic Curve Cryptography*, Ubiquity, **2008** No. 7 (2008).
- [5] K. Lauter, *The Advantages of Elliptic Curve Cryptography for Wireless Security*, *IEEE Wireless communications*, **11** Issue 1 pp. 62-67 (2004).
- [6] R. Impagliazzo, M. Luby, *One-way functions are essential for complexity based cryptography*, *Foundations of Computer Science 1989. 30th Annual Symposium on Research Triangle Park NC*, pp. 230-235 (1989).
- [7] D. Giry, *BlueKrypt - v 29.2*, <https://www.keylength.com/en/8/>, Sept 2015.
- [8] P. Krawczyk (2001), *Microsoft's Digital Rights Management Scheme-Technical Details*, <http://cryptome.org/ms-drm.htm>
- [9] E. W. Weisstein, *Elliptic Curve Group Law*. MathWorld—A Wolfram Web Resource. <http://mathworld.wolfram.com/EllipticCurveGroupLaw.html>
- [10] I. Blake, G. Seroussi; N. Smart (2000). *Elliptic Curves in Cryptography*. LMS Lecture Notes. Cambridge University Press. ISBN 0-521-65374-6.
- [11] A. J. Menezes, T. Okamoto, S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, *IEEE Transactions on Information Theory*, **39**, Issue 5 pp. 1639-1646 (1993).
- [12] N. P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, *Journal of Cryptology*, **12**, Issue 3 pp. 193-196, (1999).
- [13] W. Diffie, M. Hellman, *New directions in cryptography*, *IEEE Transactions on Information Theory*, **22**, Issue 6, pp. 644 - 654 (1976).
- [14] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, *Elliptic Curve Cryptography in Practice*, *Lecture Notes in Computer Science*, **8437**, pp. 157-175 (2014).
- [15] D. Naylor, A. Finamore, I. Leontiadis, Y. Grunenberger, M. Mellia, M. Munafo, K. Papagiannaki, P. Steenkiste, *The Cost of the "S" in HTTPS*, *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, pp. 133-140 (2014).
- [16] M. Laska, *An Algorithm for Finding a Minimal Weierstrass Equation for an Elliptic Curve*, *American Mathematical Society*, **38**, No. 157 pp. 257-260, (1982).
- [17] I. Connell (1999), *Elliptic Curve Handbook*. This handbook is a set of notes of about 540 pages, which can be found at the address: <https://pendientedemigracion.ucm.es/BUCM/mat/doc8354.pdf>.
- [18] D. Johnson, A. Menezes, S. Vanstone, *The elliptic curves digital signature algorithm (ECDSA)*, *International Journal of Information Security*, **1**, Issue 1, pp.36-63 (2001) - First Online: 31 Jan 2014.